§170.315(e)(3) Patient health information capture

2015 Edition CCGs

Version 1.4 Updated on 06-15-2020

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-22-2015
1.1	Design and Performance: Removed “Safety-enhanced design (§ 170.315(g)(3)) must be explicitly demonstrated for this criterion”.	11-13-2015
1.2	Clarification recommending developers consider whether additional security protections are needed if patient provided health information is saved to an end-user device, but it is not required for certification.	01-05-2016
1.3	Clarifications on the "linking" requirement.	07-06-2016
1.4	Updated the Security requirements per 21st Century Cures Act.	06-15-2020

Regulation Text

Regulation Text

§170.315 (e)(3) *Patient health information capture—*

Enable a user to:
(i) Identify, record, and access information directly and electronically shared by a patient (or authorized representative).
(ii) Reference and link to patient health information documents.

Standard(s) Referenced
None

Certification Companion Guide: Patient health information capture

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 2015 Edition final regulation. It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
New	No	Not Included	Yes

Certification Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(e)(3). As a result, an ONC-ACB must ensure that a product presented for certification to this criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be presented once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) "VDT" and (e)(2) "secure messaging," which are explicitly stated.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

Table for Privacy and Security

- If choosing Approach 1:
  - Authentication, access control, and authorization (§ 170.315(d)(1))

- Auditable events and tamper-resistance (§ 170.315(d)(2))
- Audit reports (§ 170.315(d)(3))
- Automatic access time-out (§ 170.315(d)(5))
- Emergency access (§ 170.315(d)(6))
- End-user device encryption (§ 170.315(d)(7))
- Encrypt authentication credentials (§ 170.315(d)(12))
- Multi-factor authentication (MFA) (§ 170.315(d)(13))

- If choosing Approach 2:
  - For each applicable P&S certification criterion not certified for Approach 1, the health IT developer may certify using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces the Health IT Module to access external services necessary to meet the requirements of the P&S certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* Final Rule at 85 FR 25710 for additional clarification.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- There is no standard required for this certification criterion.
- This criterion replaces the 2014 Edition "advance directives" certification criterion (§ 170.314(a)(17)) and applies to various patient health information documents. [see also 80 FR 62661]
- We encourage health IT developers to develop innovative and efficient ways to meet this criterion and simultaneously support providers accepting health information from patient. [see also 80 FR 62662]
- Although the privacy and security requirements described above do not require that a privacy and security certification criterion must be explicitly tested with this functionality at § 170.315(e)(3), Health IT Module developers should perform their own security risk assessment to determine if additional security protections are necessary. For example, if a Health IT Module requires that a user first save a patient-supplied document to their end-user device before capturing the information, developers should consider adding end-user device encryption to protect this data. However, this

functionality is not required to meet the privacy and security requirements for certification, but is strongly recommended.

Paragraph (e)(3)(i)

Technical outcome – A user can identify, record, and access information directly and electronically shared by a patient.

Clarification:

- The intent of this provision is to establish at least one means for accepting patient health information directly and electronically from patients in the most flexible manner possible. [see also 80 FR 62662]
- The criterion does not seek to define the types of health information that could be accepted as we believe this should be as broad as possible and could be documents or health information from devices or applications. The devices and applications could include home health or personal health monitoring devices, fitness and nutrition applications, or a variety of other devices and applications. In addition, patient health information could be accepted directly and electronically through a patient portal, an API, or even email. [see also 80 FR 62662]
- "Identify," by example, means labeling health information documents as "advance directives" or "birth plans." [see also 80 FR 62662]
- "Record," means the ability to capture and store. [see 80 FR 62610; see also 77 FR 54168]
- "Access," means the ability to examine and review. [see 80 FR 62610; see also 77 FR 54168]

Paragraph (e)(3)(ii)

Technical outcome – A user can reference and link to patient health information documents.

Clarification:

- "Reference" requires providing narrative information on where to locate a specific health information document. [see also 80 FR 62662]
- "Linking" requires a Health IT Module to demonstrate it could link, via the internet, to an external site/source storing a health information document(s). While an intranet link to a health information document might suffice for provider use, a Health IT Module will still need to demonstrate the ability to link to an external site via the internet or external storage source.
  - The criterion does not define how and to what the health IT links (e.g., Dropbox, another health IT developer's patient health record, a state advance directive repository, etc.). However, linking to an integrated portal would not suffice.
  - The requirement of this provision does not go beyond the specified functionality such as demonstrating the log-in/authentication process in connection with linking, via the internet, to an external site/source. [see also 80 FR 62662]
  - This requirement is separate and distinct from the criterion's requirement that health IT be able to demonstrate that it can access information directly and electronically shared by a patient (paragraph (e)(3)(i)).

Content last reviewed on June 23, 2020